

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

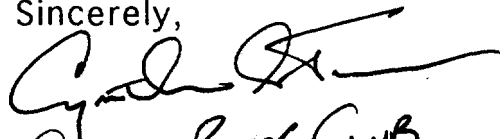
The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the;

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXC's and LEC's to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll Fraud is a financially devastating problem that effects the entire **telecommunications** industry including users, vendors and carriers. I am sure, that if we all work together we can and will make a positive impact on this problem.

Sincerely,

  
Gerald St. John  
Telecom MGR

January 11, 1994

Mr. William F. Canton  
Acting Secretary  
Federal Communications Commission  
1919 M Street NW  
Washington, DC 20554



Re: CC Docket no. 93-292

Dear Mr. Canton:

I am a telecommunications professional who is responsible for my company's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXCs, LECs and CPE vendors. The legal obligations of the IXCs, LECs and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXCs (Sprint Guard™, MCI Detect™, and AT&T Netprotect™) and insurance companies are too expensive. Monitoring and proper notification by the IXCs must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LECs must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

No. of Copies rec'd  
List ABCDE

*Orig*

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the;

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXC's and LEC's to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll Fraud is a financially devastating problem that effects the entire telecommunications industry including users, vendors and carriers. I am sure, that if we all work together we can and will make a positive impact on this problem.

Sincerely,



*Anthony Martin, Vice Communications*

*Toll Boston Company*

## CARPENTER TECHNOLOGY CORPORATION

GENERAL OFFICE

P.O. BOX 14662, READING, PA 19612-4662 • (215) 208-2000



RECEIVED

JAN 11 9 1994

January 11, 1994 MAIL ROOM

Mr. William F. Canton  
Acting Secretary  
Federal Communications Commission  
1919 M Street NW  
Washington, DC 20554

RE: CC DOCKET NO. 93-292

Dear Mr. Canton:

As a Telecommunications professional, I realize that although I may reduce the risk, no matter how many steps I take to secure the systems I am responsible for, I am still vulnerable to toll fraud.

IXC's, LEC's and CPE vendors need incentive to encourage them to help reduce and eliminate toll fraud. Without that incentive, the costs of toll fraud will continue to fall on the PBX owners.

Although some IXC's and insurance companies offer "monitoring and notification programs" most are too expensive and are barely more than an opportunity for them to sell additional products and services. Monitoring and notification of toll fraud should be part of vendors basic offerings at no additional cost to the customer.

All CPE equipment should be delivered with explicit warnings about the risks of toll fraud as they specifically relate to that product and without standard default passwords. Security hardware should be included during the assembly of the equipment and always part of even the most basic package.

We must all take some responsibility for the problem of toll fraud. If toll fraud occurs due to negligence of one or more parties, then any financial loss should be equitably distributed among those parties. If there is no negligence, than the loss needs to be shared equally by all parties, but repayable by those who committed this crime after their conviction.

The sad story is that with the crime of toll fraud, the victim is the one who is "punished".

Sincerely,

Robin C. Wenger  
Supervisor-  
Telecommunications

None of Copies rec'd  
List ABCDE

**JOHN DEERE LIFE INSURANCE COMPANY**

JOHN DEERE CENTRE, 300 E. STATE STREET, JACKSONVILLE, IL 62650-2030  
217/245-9531 TOLL FREE 800/637-4475

10 January 1994

**RECEIVED****JAN 19 1994****FCC MAIL ROOM**

Mr. William F. Canton  
Acting Secretary  
Federal Communications Commission  
1919 M Street NW  
Washington, D.C. 20554

RE: CC Docket 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for my company's communications systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we do not control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided IXCs, LECs and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs and CPEs who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later.

While the programs offered by IXCs, such as MCI Detect, AT&T NetProtect and Sprint Guard have broken new ground in relation to



AFFILIATED COMPANIES  
JOHN DEERE INSURANCE COMPANY  
JOHN DEERE INSURANCE COMPANY OF CANADA  
JOHN DEERE TRANSPORTATION SERVICES, INC.  
ROCK RIVER INSURANCE COMPANY  
SIERRA GENERAL LIFE INSURANCE COMPANY  
TAHOE INSURANCE COMPANY

No. of Copies rec'd Orig.  
List ABCDE

preventing toll fraud, they still do not do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXCs should be a part of the basic interexchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXCs were monitoring all traffic, there would not be any cases of toll fraud for periods longer than a day. As hackers begin new methods of breaking into systems by using local lines instead of 800 numbers, the LECs should be required to offer monitoring services similar to the IXCs.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXCs and LECs to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally. However, shared liability only addresses the symptom of the problem of toll fraud and not the cause.

The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only "hack" to gain knowledge. If this were the case, there would not be a toll fraud problem. While it is the hacker who breaks into the systems and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Sincerely,



THOMAS D. NEWBY  
System Administrator